

AB:PP

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
ONE LG CELLULAR DEVICE, MODEL
LM-X212TA, IMEI NUMBER 356351-09-
606690-4

APPLICATION FOR A SEARCH
WARRANT FOR AN ELECTRONIC
DEVICE

Case No. 20-MJ-86

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, LUANNE WALTER, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with Homeland Security Investigations (“HSI”). I have been a federal law enforcement officer since 2001. My responsibilities include investigations of cases involving the promotion of a sexual performance by a child through the use of electronic devices and the internet, possession and distribution of child pornography through the use of electronic devices and the internet, as well as dissemination of indecent material to minors, and other incidents of the exploitation of children on the internet. I have gained expertise in this area through training in classes and daily work

related to conducting these types of investigations. As part of my responsibilities, I have been involved in the investigation of numerous child pornography and child exploitation cases.

3. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: my personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

4. HSI is investigating the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched is an LG CELLULAR DEVICE, MODEL LM-X212TA, IMEI NUMBER 356351-09-606690-4, hereinafter the "Device." The Device is currently in the custody of HSI within the Eastern District of New York.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

8. On November 28, 2012, Robert Smith pled guilty before the Honorable Cheryl L. Pollak to possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). See United States v. Smith, 11-CR-156. Subsequently, the Honorable Nicholas G. Garaufis, sentenced Smith to 48 months' imprisonment to be followed by five years of supervised release.

9. As part of his sentence, Judge Garaufis imposed numerous special conditions of release. As relevant to this application, the Court imposed the following condition:

THE DEFENDANT SHALL ALSO COOPERATE WITH THE U.S. PROBATION DEPARTMENT'S COMPUTER AND INTERNET MONITORING PROGRAM. COOPERATION SHALL INCLUDE, BUT NOT LIMITED TO, IDENTIFYING COMPUTER SYSTEMS, INTERNET CAPABLE DEVICES, AND/OR SIMILAR ELECTRONIC DEVICES THE DEFENDANT HAS ACCESS TO, AND ALLOWING THE INSTALLATION OF MONITORING SOFTWARE/HARDWARE ON SAID DEVICES, AT THE DEFENDANT'S EXPENSE. THE DEFENDANT SHALL INFORM ALL PARTIES THAT ACCESS A MONITORED COMPUTER, OR SIMILAR ELECTRONIC DEVICE, THAT THE DEVICE IS SUBJECT TO SEARCH AND MONITORING. THE DEFENDANT MAY BE LIMITED TO POSSESSING ONLY ONE PERSONAL INTERNET CAPABLE DEVICE, TO FACILITATE THE PROBATION DEPARTMENT'S ABILITY TO EFFECTIVELY MONITOR HIS INTERNET RELATED ACTIVITIES. THE DEFENDANT SHALL ALSO PERMIT RANDOM EXAMINATIONS OF SAID COMPUTER SYSTEMS, INTERNET CAPABLE DEVICES, SIMILAR ELECTRONIC DEVICES, AND RELATED COMPUTER MEDIA, SUCH AS CD'S, UNDER HIS CONTROL.

10. On or about July 31, 2019, Smith reported to a Probation Officer with the U.S. District Court for the Eastern District of New York that he did not possess a smart phone or any other internet capable device.

11. On or about September 25, 2019, the Probation Officer visited Smith's residence in Brooklyn, New York. The Probation Officer asked Smith whether he possessed a smart phone and Smith responded that he did. Smith then produced the Device. Smith's possession of the Device violated the terms of his Supervised Release, because, inter alia, he did not identify this Device for the Probation Department, and accordingly, there was no monitoring software on the Device as required by the terms of his supervised release. The Probation Officer told Smith that he needed to relinquish the Device and provide his passcode, which Smith did.

12. On or about October 24, 2019, a Probation Officer conducted a cursory search of the Device. The Probation Officer located searches indicating that pornography had been viewed on the Device, which additionally violated a different term of supervised release which prohibited Smith from using an internet capable device of "access[ing] pornography of any kind." Although the Probation Officer did not locate any child pornography, he did find searches or videos containing terms such as "teen," "lil" and "young." The Probation Department subsequently provided the Device to HSI.

13. On or about November 27, 2019, Smith admitted to his Probation Officer that he viewed child pornography on the Device, specifically images of female children between eight to ten years old. Smith said that he had obtained the Device in approximately May 2019 and that he had viewed child pornography on approximately 50 separate occasions since then.

14. As discussed above, the Device was taken from Smith by the Probation Department and is currently in the lawful possession of the HSI within the Eastern District of

New York. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

15. Although the Probation Department did not locate any child pornography on the Device, based on my training and experience I know that the forensic search of the Device that is sought herein is significantly more comprehensive than a cursory search that an individual can do by simply opening and reviewing the device. For example, a forensic search will comprehensively search the entire device for child pornography as permitted by the warrant, and can locate files that have been deleted, as well as other evidence that files, such as child pornography, have been viewed or searched for that could constitute evidence of a violation of 18 U.S.C. § 2252A.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice

communications, wireless telephones offer a broad range of capabilities.

These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store

other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

21. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

22. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



LUANNE WALTER

Special Agent

United States Department of Homeland Security,
Homeland Security Investigations

Sworn to before me this
24th day of January, 2020



THE HONORABLE CHERYL L. POLLAK
CHIEF UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

1. The property to be searched is the property to be searched is an LG CELLULAR DEVICE, MODEL LM-X212TA, IMEI NUMBER 356351-09-606690-4, hereinafter the "Device." The Device is currently in the custody of HSI within the Eastern District of New York. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 2252, and 2252A from April 1, 2019 to September 26, 2019, including:
 - a. images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation 18 U.S.C. §§ 2252 and 2252A, in any form wherever they may be stored or found;
 - b. motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
 - c. records and information pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct;
 - d. records and information concerning any Internet accounts used to possess, receive or distribute child pornography; and
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
 - a. records of Internet Protocol addresses used;

- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.